AFRL-RI-RS-TR-2017-040

US CYBER CHALLENGE RESEARCH

NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS (NBISE)

FEBRUARY 2017

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2017-040 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
FRANCES A. ROSE
Work Unit Manager

/ S /
JOHN D. MATYJAS
Technical Advisor, Computing
and Communications Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
FEBRUARY 2017	FINAL TECHNICAL REPORT	APR 2012 – AUG 2016

4. TITLE AND SUBTITLE

US CYBER CHALLENGE RESEARCH

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA8750-12-2-0120

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Karen Evans

5d. PROJECT NUMBER
USCC

5e. TASK NUMBER
12

5f. WORK UNIT NUMBER
FR

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
National Board Of Information Security Examiners (NBISE)
1700 N Moore St, Ste 2100
Arlington, VA 22209-1922

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RITE
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2017-040

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The goal of this research project is to develop, test, analyze and assess cybersecurity tactical and strategic gaming competitions to determine the ability to defend the nation's critical infrastructure; ability to mitigate damage; and success in implementing defensive tactics to prevent future attacks. This project will develop, test, evaluate and assess alternative methods for identifying computer security talent that will be able to identify threats and improve our country's ability to anticipate, avoid, detect and defeat cyber threats.

15. SUBJECT TERMS
Cyber Challenge, CCX Platform, NICE Program, USCC

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**FRANCES ROSE**
U	U	U	UU	34	19b. TELEPHONE NUMBER (*Include area code*) **N/A**

TABLE OF CONTENTS

Section **Page**

List of Tables

List of Figures

1.0 SUMMARY

The 2012 World Economic Forum declared data an economic asset similar to gold or currency. With ninety percent of the world's data being created in the last two years, the challenge to provide adequate security is ever increasing. Meeting the demand for top technical cybersecurity talent is one of the continuing challenges facing military and civilian government leaders. On July 12, 2016, the White House launched the first ever Federal Cybersecurity Workforce Strategy.[1] Competitions continue to provide promising avenues for identification of future talent, for ranking candidates on cyber skills, and for motivating candidates to become fully committed to advancing their skills in cybersecurity. The US Cyber Challenge (USCC) is one of the initiatives to address this workforce gap by developing the next generation of cyber experts through education and hands-on defense gaming strategies. The USCC participated in the White House Cybersecurity Competition Workshop hosted by the Office of Science and Technology Policy on July 27, 2016.[2]

By creating excitement and highlighting competitors' successes, the USCC continues to develop various avenues to communicate the following:

- There are cool jobs in technology;
- Organize highly selective summer camps;
- Ensure the public knows how impressive it is to be selected to participate; and
- Analyze what works and what does not work in each of these areas.

During the period of performance, April 2012 through August 2016, the USCC held several competitions and challenges and also developed the assessment framework to categorize competitions mapping them to the National Initiative for Cybersecurity Education (NICE) and providing the platform for social interaction with the cybersecurity competition participants with themselves and with future employers. The impact of the USCC is being measured against the participation in this platform called, CyberCompEx.org (CCX) as well as our future participation with employers to engage with the participants. Currently, CCX has the following:

Table 1: Current Statistics from CyberCompEx.org

Community Members	2,191
Total Topics	136
Total Topic Replies	86
Total Blog Posts	29
Total Clips	325

In summary, the USCC continues our outreach and partnerships using the social media and other communications capabilities as well the resources of the Center for Internet Security to include the Multi-State ISAC community to increase the overall numbers of participations while working with partners such as Life Journey with their 5 million members to broaden the information and participation in CCX using the tools developed for individuals to be able to better communication their skill sets to potential employers to reduce the cybersecurity workforce gap.

2.0 INTRODUCTION

In October 2016, the NICE program released the heat map of the location of the cybersecurity jobs (http://www.cyberseek.org).[4] The data states there are 348,975 vacancies in the United States alone. The Center for Strategic and International Studies (CSIS) in partnership with Intel Security released, "Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills," on July 27, 2016. This study surveyed eight countries, which highlights the need for employers to play in recruiting, retaining, and training their workforce.[3] On November 1, 2016, the USCC participated in the official release of the white paper on the role of cybersecurity competitions in workforce development where the USCC team participated in the development through the Summer of 2016. [5]

The Council on CyberSecurity (formerly the National Board for Information Security Examiners), U.S. Cyber Challenge (USCC), continues to develop partnerships to maintain the CCX platform for continuous engagement outside of the competitions and summer camps to highlight career paths for individuals to obtain the high-level technical skills required for meaningful employment. USCC believes the path must be available through various levels of engagement and throughout an individual's career. Finally, the USCC continues to believe performance metrics should be developed in order to measure the progress being made to reduce the risk for the national critical infrastructure regarding cyber threats.

The USCC mission continues to be the search for 10,000 Americans with the skills to fill the ranks for the cybersecurity practitioners, researchers, hunters and warriors. Specifically, USCC objectives are to:

1. **Identify:** increase cybersecurity knowledge and talent self-awareness among high school students, college age students, current professionals and other interested persons who are looking to enter into the cyber security professional ranks and/or further their existing careers;
2. **Engage:** engage individuals in order to increase the talent pool for cybersecurity professionals, in both the public and private sectors. This objective includes engaging individuals across various demographics, including women and minorities; and
3. **Challenge:** provide opportunities for skill development through cybersecurity competitions and pathways to provide increasingly difficult challenges and competitions as well as provide access to educations, resources, mentoring, scholarships, internships and job opportunities.

With the development of the CCX platform, the USCC has the ability to receive continuous feedback to continually improve on these objectives and the collection of the necessary data as well as establishing the data elements, conducting appropriate collection activities and analysis, and addressing the challenges for our on-going efforts.

3.0 METHODS, ASSUMPTIONS, AND PROCEDURES

3.1 Assumptions

With the initial work conducting the USCC used the initial assessment framework developed under this research proposal, there a number of important assumptions. These assumptions are as follows:

- A more cybersecurity aware populous will mitigate against the Nation's cyber risks and improve the Nation's cybersecurity posture.
- Individuals with the right skills and education in cybersecurity, in the appropriate federal and industry roles and positions, will improve the cyber security posture of the Nation/National critical information technology (IT) infrastructure.

Given these assumptions, the initial assessment framework does not focus on assessing or quantifying the Nation's cyber risk profile or cyber risk posture as this is done at the national level and continues to be expanded by reports provided by the national intelligence community. The initial assessment framework was designed to assess and improve the activities of the USCC and the cybersecurity professional activities in-line with the objectives of *identify, engage* and *challenge*.

Furthermore, the initial assessment framework was designed to support the underlying USCC's "pathway" construct. In this construct, the field of cybersecurity is viewed as a pathway with multiple entry and exit points, as well as, various paths to differing destinations for education and eventual job entry or if you are already in the job market, re-entry for developmental purposes to become more cyber-enhanced and/or a cybersecurity professional. However, since this initial framework was developed and used by the USCC, the analogy of a "roadway" with on and off ramps works well. This allows for the USCC to represent that many may be entering the field at different points of time in their career, they may be coming from differing locations or career backgrounds, and ultimately, they may choose differing paths or specialties within the cybersecurity field. In contrast, the "pipeline" analogy continues to be unfitting the USCC approach because it implies one single point of entry and highly structured, linear path to a single destination. As such, the information on a participant's background, experience, skills, and successes to help assist and map a pathway through to their choice and the CCX platform was development with this methodology in mind.

3.2 Methods

The initial assessment framework was geared towards measuring the success of the USCC and cybersecurity professional development activities in achieving the USCC's objectives. As the USCC matured, we continued to refine the methodology and the tools. We developed two models using experts across the nation to address critical jobs at the Department of Homeland Security. The Mission Critical Role Project was the scenario-driven view of the knowledge, proficiency with tools, and abilities required for mission critical roles is a framework which we are planning to use for competition evaluation design, and to provide a way to recognize competitors who score by providing points toward their user profile and/or user reputation index. The successful competitor would demonstrate possession of the knowledge required by a specific competition, working proficiency for the tools needed to compete and the underlying abilities exercised. The 'ground truth' scenario-based job competency definitions for mission critical roles for advanced threat response (Security Monitoring and Event Analyst) and for operational security testing (System and Network Penetration Tester) were developed and

released to the public.

3.3 Procedures

After deploying the initial assessment framework, the USCC moved towards continuous development and feedback cycle as depicted by:

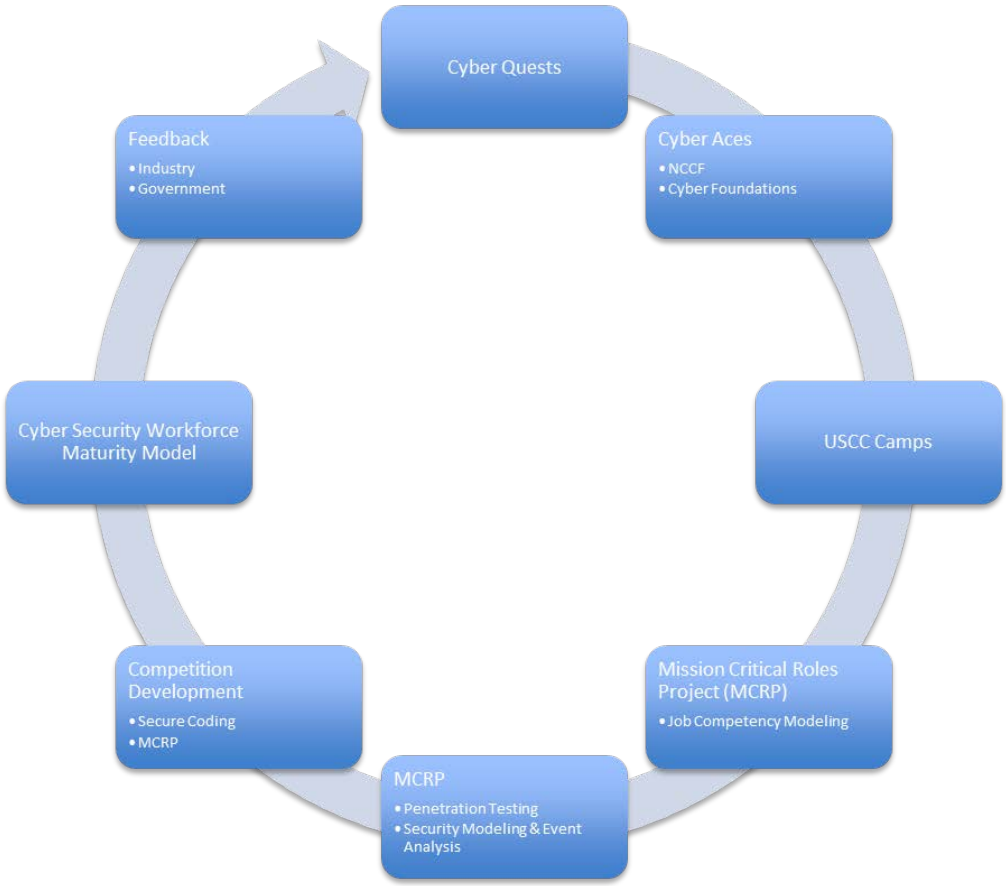


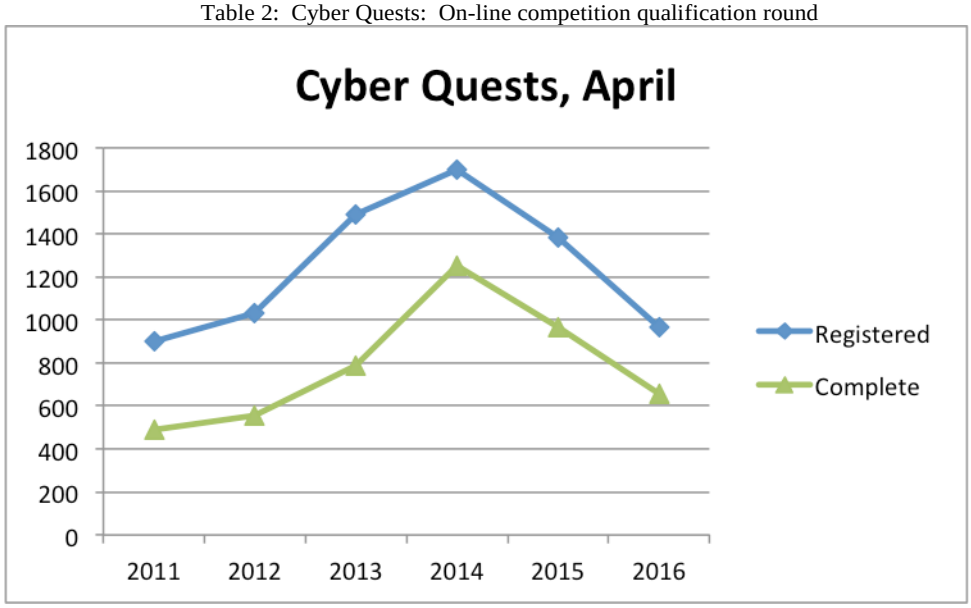
Figure 1: Development Cycle for USCC Activities and Partnerships

4.0 RESULTS AND DISCUSSION

The Cyber Camps provide crucial skills development and enable USCC to tap into the tremendous talent across our nation to identify those with a passion for security and a desire to put their skills to good use in addressing our Nation's cyber security workforce challenges. In addition to providing expert training for participants to improve their skills and marketability, the Cyber Camps provided attendees the opportunity to engage with major technology companies and government agencies at onsite job fairs for scholarship, internship and employment opportunities as well as engage industry professionals in an ethics panel.

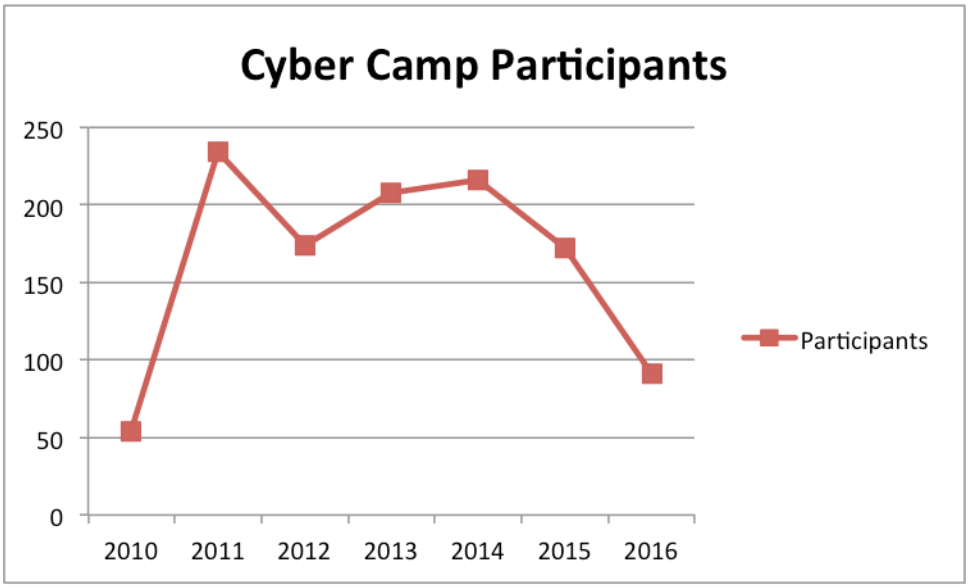
The camps continue to be "invitation only" after students initially completed the on-line competition, Cyber Quest. Furthermore, the camps were provided as either day camps or in-residence overnight camps. For the overnight camps, there was a minimum age requirement of 18 years and older.

Table 2: Cyber Quests: On-line competition qualification round



The Cyber Quests chart illustrates the competition used for the qualification for the camps only. The USCC in conjunction with our partners from CounterHackers developed multiple competitions and they were conducted during various times throughout the year. The qualifying competition for the camps ran during the April time period each year. The two years of declining data are explained by our focus on completion and shortened the competition time period. We concluded on the date specified and did not extend the last two years. What we have observed is the participants wait until the last minute to compete. They anticipated we would extend the dates to increase the participation rates and we did not. We did receive feedback and requests to extend each year of those two years.

Table 3: USCC Camps



The overall camp participation rate illustrates several findings. For example, in 2011, the USCC conducted 6 camps including one at the high school level. We developed and personally invited all the participants. The low number in 2016 is the result of only three camps being conducted. The decline in 2015 and the 2016 are directly attributed to our partner, Virginia Tech. They had new staff who took ownership of all aspects of the camps. With this ownership, the local lead delegated the work and the invitations did not get sent out to the potential camp participants. Also, Virginia Tech did not conduct a camp in 2016 due to local staffing issues. The USCC continued to opt for quality verses quantity.

4.1 Social Media Statistics for August 2016

Facebook: August 1, 2016 – August 31, 2016

Total Likes = 1,887 Total (growth of +0.2%)

New Likes = 11

Weekly Total Reach = 31

Wall Posts (from fans) = 10 Posts

Post Feedback = 50 Likes, 2 Comments & 16 Shares

Gender Summary = 78% Male; 21% Female; 1% Unknown

Twitter:	July 31	-	2,158 Followers
	August 31	-	2,196 Followers (growth of +1.8%)
LinkedIn:	July 31	-	1,324 Members
	August 31	-	1,324 Members (growth of 0%)

USCyberChallenge.org: Total Visitors = 1,433

Unique Visitors = 1,255

Page Views = 2,426

CyberCompEx: August Registration = 89

Twitter Followers: 146

4.2 2016 Capture the Flag (CTF) Summary

In previous USCC summer camps, Capture the Flag (CTF) environments were built with support of various sponsors which while successful were deemed not to be a scalable CTF environment. As a result, USCC explored the question 'which virtual environment should be used for the "Capture the Flag (CTF)" for the camps? And what should be the partnership(s) for the future?' The USCC through the years used multiple platforms primarily with ThreatScapeand then this past year with the Michigan Range. The CTFs also only tracked overall team performance. The USCC saw the need for the individual's contribution to the team performance. The following highlights the results of the testing of the engine we used during the CTF competitions at the camps.

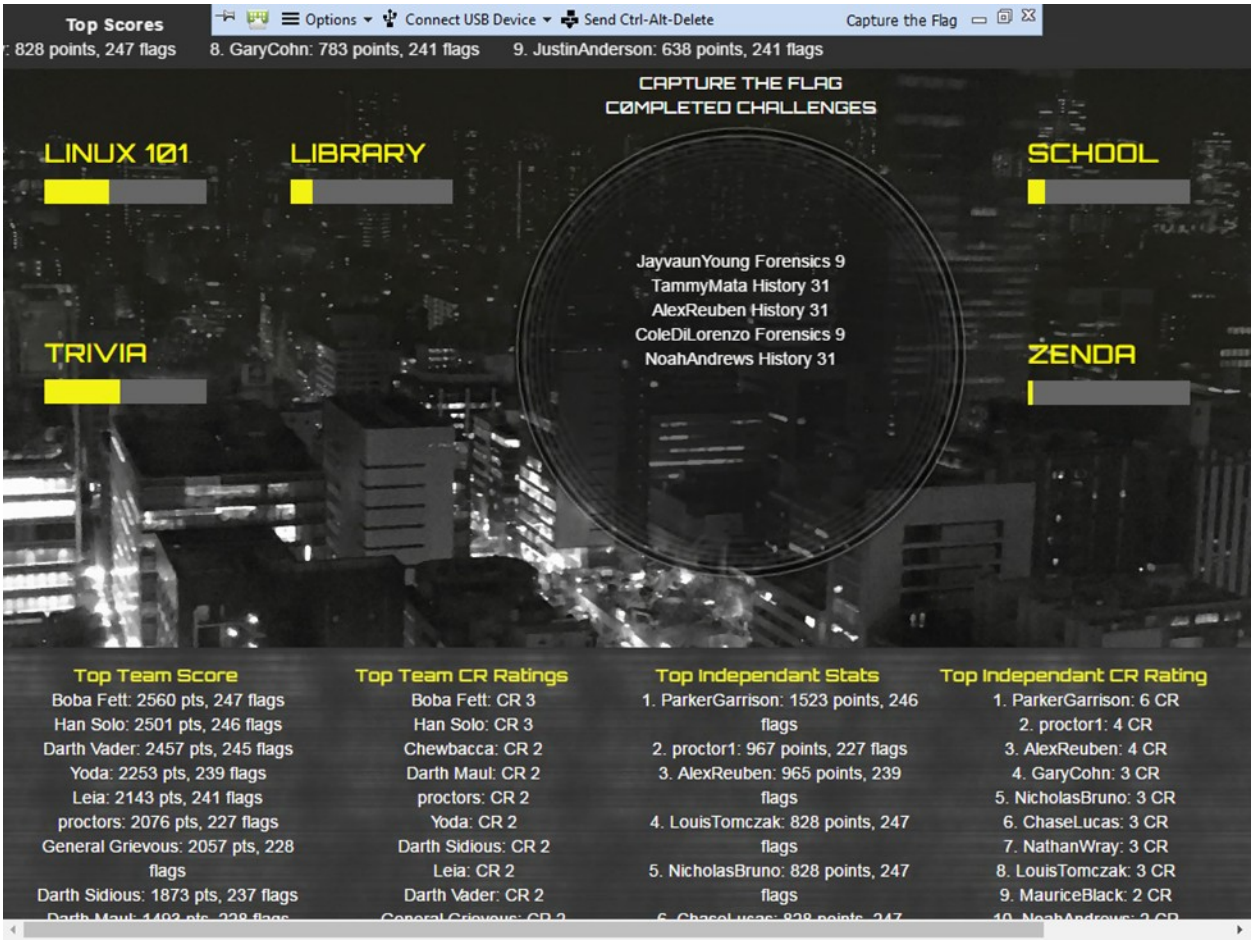


Figure 2: CTF Display from the Delaware 2016 Camp

4.3 2016 Camp Summary

The report provides an overview of the feedback collected from camp surveys, a summary of findings from interviews with camp administrators, teaching assistants (TAs) and instructors, a summary of overarching observations derived from those interviews, as well as general recommendations for future camps. Since the inception of the camps, the USCC has refined the data collection mechanisms. The full report is included as Appendix B, US Cyber Challenge 2016 Camp Analysis. The following is the overall summary of the data from the three camps held in Delaware, Moraine Valley and Southern Utah.

Comprehensive Course Analysis Results

Number of Respondents

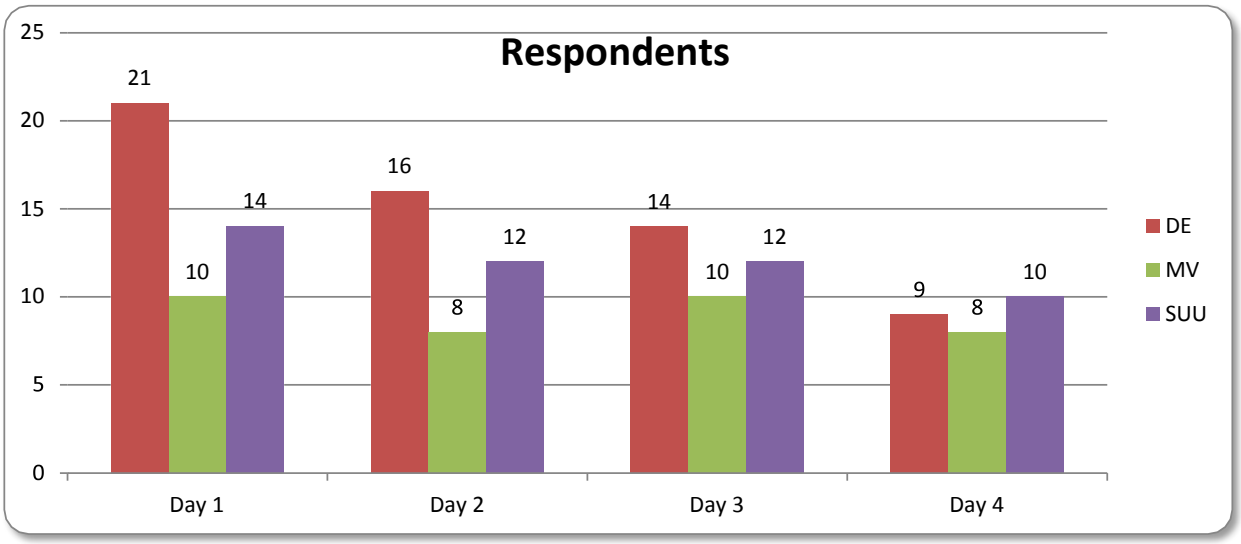


Table 4: 2016 Camp Summary from CCX

Respondent Summary			
	DE	**MV**	**SUU**
Day 1	21	10	14
Day 2	16	8	12
Day 3	14	10	12
Day 4	9	8	10

4.4 CyberCompEx.org

There are other employment platforms competing with CyberCompEx.org however, the key to our success is our partnership with Monster.com. The overall goal is to have the competitions be of value to the individual as they build out their profiles and navigate their career options on the CCX and to provide value to the employers in order for them to find potential employees who have demonstrated the skills needed to perform on the job. The pilot for employers was conducted with SANS Institute and we are continuing this effort going forward. Currently, we have over 12 pending requests from employers to participate on CCX.

Figure 3: Screen shot of CCX including our partnership with SANS for the Talent Connection

5.0 CONCLUSIONS

The success of this effort and the CCX platform is dependent on the continual flow of data from user participation. Although there is likely a small population with an innate interest in continued participation over time, long-term analysis benefits from the 'pathway' model of incremental steps to include activities, education, achievement, and ultimately a benefit, which is the continual achievement and success yielding a payout or benefit to the participating individual. Our on-going partnerships with the schools for the camps, with associations such as AFFIRM for business models to support the camps' scholarships, Monster.com for CCX, Amazon Web Services for the platform for the USCC website, Life Journey for education outreach, and others will ensure the on-going sustainability of the various models in place.

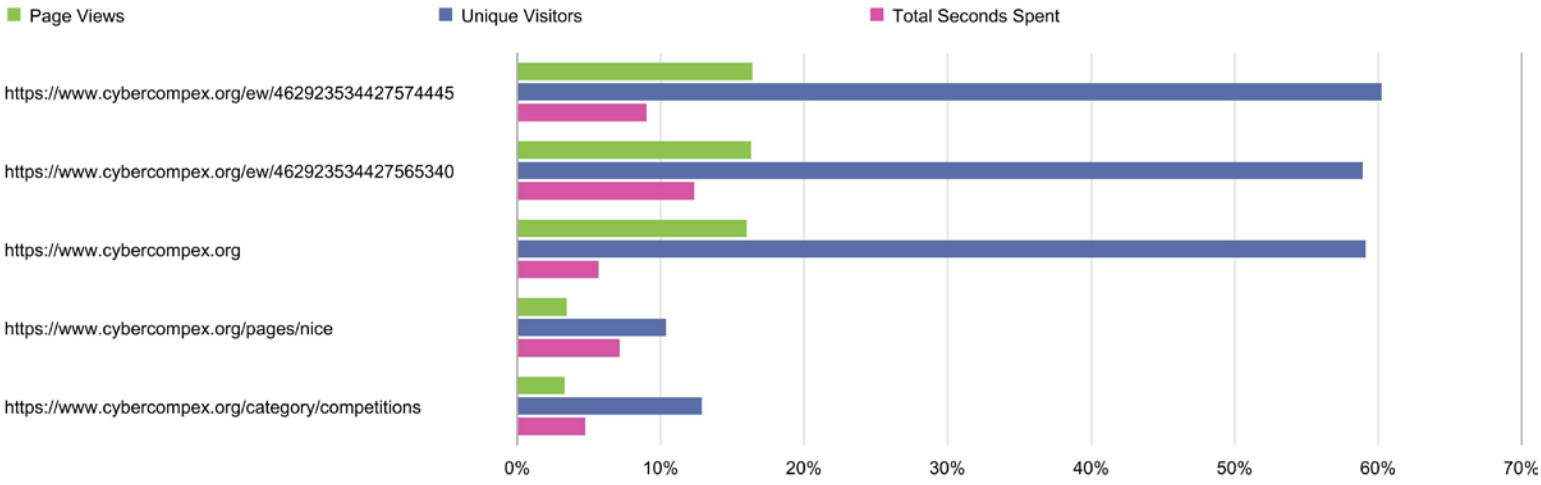
The USCC will continue to use the social media capabilities and other communications capabilities as well the resources of the Center for Internet Security to include the Multi-State ISAC community to increase the overall numbers of participants on CCX while outreaching to potential employers.

6.0 REFERENCES

1. https://www.whitehouse.gov/blog/2016/07/12/strengthening-federal-cybersecurity- workforce
2. https://www.whitehouse.gov/blog/2016/07/27/building-workforce-through- cybersecurity-competitions
3. "Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills," on July 27, 2016. https://newsroom.intel.com/press-kits/hacking-skills-shortage/
4. http://cyberseek.org/heatmap.htmlThe role of cybersecurity competitions in workforce development https://www.cybercompex.org/clip/cybersecurity-games-building-tomorrow-s-workforce
5. Federal Cybersecurity Workforce Strategy, dated July 12, 2016 https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf

Report Type: Ranked
Selected Metrics: Page Views & Unique Visitors & Total Seconds Spent
Correlation Filter: None
Data Filter: None

Compare to Report Suite: None
Compare to Segment: None
Percent Shown as: Number



Pages Report | All Visits (No Segment) | August 2016 | Graph generated by Adobe Analytics at 9:23 AM EDT, 1 Sep 2016

	Page	Page Views		Unique Visitors		Total Seconds Spent	
1.	https://www.cybercompex.org/ew/462923534427574445	1,205	16.4%	603	60.2%	18,985	9.0%
2.	https://www.cybercompex.org/ew/462923534427565340	1,199	16.3%	590	58.9%	26,034	12.3%
3.	https://www.cybercompex.org	1,175	16.0%	592	59.1%	11,953	5.7%
4.	https://www.cybercompex.org/pages/nice	254	3.5%	104	10.4%	15,053	7.1%
5.	https://www.cybercompex.org/category/competitions	243	3.3%	129	12.9%	10,040	4.8%
6.	https://www.cybercompex.org/tos	218	3.0%	143	14.3%	5,753	2.7%
7.	https://www.cybercompex.org/join	171	2.3%	121	12.1%	2,033	1.0%
8.	https://www.cybercompex.org/groups	114	1.6%	49	4.9%	2,783	1.3%
9.	https://www.cybercompex.org/member-cp/create-private-message	92	1.3%	2	0.2%	1,271	0.6%
10.	Other	79	1.1%	15	1.5%	3,297	1.6%
11.	https://www.cybercompex.org/forums	78	1.1%	48	4.8%	583	0.3%
12.	desktop|ccx|hiring|/login.aspx	76	1.0%	32	3.2%	2,763	1.3%
13.	https://www.cybercompex.org/login	74	1.0%	61	6.1%	996	0.5%
14.	https://www.cybercompex.org/pages/about	46	0.6%	32	3.2%	1,971	0.9%
15.	https://www.cybercompex.org/topic/about-cyber-grand-challenge	41	0.6%	28	2.8%	1,438	0.7%
16.	desktop|ccx|jcm|/jcm/candidates/index.aspx	38	0.5%	1	0.1%	2,512	1.2%
17.	desktop|ccx|jcm|/jcm/candidates/sendletter.aspx	38	0.5%	1	0.1%	1,274	0.6%
18.	https://www.cybercompex.org/login!login	37	0.5%	18	1.8%	1,035	0.5%
19.	https://www.cybercompex.org/category/archived-competitions	36	0.5%	28	2.8%	1,484	0.7%
20.	desktop|ccx|jpw|/jpw/jobs/index2.aspx	36	0.5%	1	0.1%	4,095	1.9%
21.	https://www.cybercompex.org/login/context/GENERAL/redirect/https%3A%2F%2Fwww.cybercompex.org%2Fq%2Fsans	33	0.4%	24	2.4%	542	0.3%
22.	https://www.cybercompex.org/member-cp/update-profile	33	0.4%	18	1.8%	3,676	1.7%
23.	desktop|ccx|mgs|/channels/mgs1000/jobsearch/powersearch.aspx	30	0.4%	8	0.8%	434	0.2%
24.	desktop|ccx|hiring|/loginjumppage.aspx	29	0.4%	10	1.0%	163	0.1%
25.	https://www.cybercompex.org/login/context/GENERAL/redirect/https%3A%2F%2Fwww.cybercompex.org%2Fcalendar	27	0.4%	21	2.1%	309	0.1%
26.	https://www.cybercompex.org/calendar	26	0.4%	19	1.9%	580	0.3%
27.	https://www.cybercompex.org/clips	25	0.3%	12	1.2%	544	0.3%
28.	desktop|ccx|jcm|/jcm/candidates/detail2.aspx	25	0.3%	1	0.1%	1,197	0.6%

	Page	Page Views		Unique Visitors		Total Seconds Spent	
29.	https://www.cybercompex.org/login/redirect/https%3A%2F%2Fwww.cybercompex.org	24	0.3%	19	1.9%	243	0.1%
30.	https://www.cybercompex.org/topic/cyberpatriot	24	0.3%	17	1.7%	1,568	0.7%
31.	desktop|ccx|hiring|/indexauthorized.redux.aspx	24	0.3%	4	0.4%	501	0.2%
32.	https://www.cybercompex.org/topic/competition-name	23	0.3%	16	1.6%	1,035	0.5%
33.	https://www.cybercompex.org/login/context/GENERAL/redirect/https%3A%2F%2Fwww.cybercompex.org%2Fclips	22	0.3%	17	1.7%	107	0.1%
34.	https://www.cybercompex.org/topic/best-online-sources-for-learning-network-security	22	0.3%	5	0.5%	1,982	0.9%
35.	https://www.cybercompex.org/topic/dc3-forensics	21	0.3%	18	1.8%	198	0.1%
36.	https://www.cybercompex.org/forum/comp-1	21	0.3%	17	1.7%	1,350	0.6%
37.	https://www.cybercompex.org/forum/code-org	21	0.3%	14	1.4%	138	0.1%
38.	https://www.cybercompex.org/topic/uscc-cyber-camps	21	0.3%	12	1.2%	844	0.4%
39.	https://www.cybercompex.org/join!execute	20	0.3%	19	1.9%	55	0.0%
40.	https://www.cybercompex.org/topic/about-cybernexs	20	0.3%	17	1.7%	1,150	0.5%
41.	https://www.cybercompex.org/members	20	0.3%	11	1.1%	564	0.3%
42.	https://www.cybercompex.org/g/sans	20	0.3%	10	1.0%	717	0.3%
43.	desktop|ccx|hiring|/order/thankyou.aspx	20	0.3%	2	0.2%	1,964	0.9%
44.	desktop|ccx|mgs|/channels/mgs1000/jobview/getjob.aspx	19	0.3%	4	0.4%	1,987	0.9%
45.	https://www.cybercompex.org/topic/code-org	17	0.2%	13	1.3%	1,771	0.8%
46.	https://www.cybercompex.org/topic/ghost-in-the-shell-code	15	0.2%	12	1.2%	1,700	0.8%
47.	https://www.cybercompex.org/forum/bsidesmsp	15	0.2%	10	1.0%	82	0.0%
48.	https://www.cybercompex.org/topic/digital-forensics-security-treasure-hunt	15	0.2%	9	0.9%	574	0.3%
49.	https://www.cybercompex.org/topic/bsidesmsp	14	0.2%	11	1.1%	613	0.3%
50.	https://www.cybercompex.org/topic/plaid-ctf	14	0.2%	10	1.0%	2,136	1.0%
51.	https://www.cybercompex.org/topic/great-camp-this-year-in-de	14	0.2%	10	1.0%	275	0.1%
52.	https://www.cybercompex.org/topic/netwars	14	0.2%	10	1.0%	195	0.1%
53.	https://www.cybercompex.org/topic/ewf-cyber-security-school-challenge	14	0.2%	9	0.9%	935	0.4%
54.	https://www.cybercompex.org/topic/network-forensic-contest	14	0.2%	7	0.7%	366	0.2%
55.	https://www.cybercompex.org/forum/training-opportunities	14	0.2%	7	0.7%	116	0.1%
56.	desktop|ccx|jpw|/jpw/jobs/selectpostings.aspx	14	0.2%	1	0.1%	174	0.1%
57.	https://www.cybercompex.org/login/context/GENERAL/redirect/https%3A%2F%2Fwww.cybercompex.org%2Fblog	13	0.2%	11	1.1%	87	0.0%
58.	https://www.cybercompex.org/topic/packetwars	13	0.2%	9	0.9%	862	0.4%
59.	https://www.cybercompex.org/topic/derbycon-ctf	13	0.2%	8	0.8%	1,765	0.8%
60.	https://www.cybercompex.org/forum/cybersecurity-tools	13	0.2%	5	0.5%	131	0.1%
61.	https://www.cybercompex.org/topic/panoply	12	0.2%	10	1.0%	769	0.4%
62.	https://www.cybercompex.org/category/tools	12	0.2%	10	1.0%	98	0.0%
63.	https://www.cybercompex.org/topic/information-security-talent-search	12	0.2%	9	0.9%	1,248	0.6%
64.	https://www.cybercompex.org/topic/overthewire-wargames	12	0.2%	8	0.8%	1,083	0.5%
65.	desktop|ccx|mgs|/channels/mgs1000/error.aspx	12	0.2%	6	0.6%	276	0.1%
66.	https://www.cybercompex.org/g/teaching-assistant-community	12	0.2%	5	0.5%	1,531	0.7%
67.	https://www.cybercompex.org/topic/ucsb-international-capture-the-flag	12	0.2%	5	0.5%	491	0.2%
68.	https://www.cybercompex.org/saml/logout	11	0.1%	11	1.1%	18	0.0%
69.	https://www.cybercompex.org/topic/defcon-crack-me-if-you-can	11	0.1%	10	1.0%	233	0.1%
70.	https://www.cybercompex.org/event/cyber-security-summit-chicago	11	0.1%	10	1.0%	177	0.1%
71.	https://www.cybercompex.org/forum/cyber-grand-challenge	11	0.1%	9	0.9%	780	0.4%
72.	https://www.cybercompex.org/topic/video-course-introduction-to-ransomware	11	0.1%	9	0.9%	226	0.1%
73.	https://www.cybercompex.org/topic/national-ccdc	11	0.1%	7	0.7%	323	0.2%
74.	https://www.cybercompex.org/topic/uscc-cyberquests	11	0.1%	7	0.7%	322	0.2%
75.	https://www.cybercompex.org/surveys	11	0.1%	7	0.7%	68	0.0%

76.	https://www.cybercompex.org/topic/ethicalhacker-net-skillz	11	0.1%	6	0.6%	459	0.2%
77.	desktop|ccx|mgs|/channels/mgs1000/resume/listresumes.aspx	11	0.1%	3	0.3%	728	0.3%
78.	https://www.cybercompex.org/login/context/GENERAL/redirect/https%3A%2F%2Fwww.cybercompex.org%2Fsaml%2Fauthn-response-form%2FrequestID%2F_681c5b76-8d44-4c87-adc3-adf369c031c7	11	0.1%	1	0.1%	1,113	0.5%
79.	https://www.cybercompex.org/topic/niccs-training-catalog	10	0.1%	8	0.8%	772	0.4%
80.	https://www.cybercompex.org/topic/mdc3	10	0.1%	8	0.8%	47	0.0%
81.	https://www.cybercompex.org/topic/isu-cyber-defense-competition	10	0.1%	7	0.7%	203	0.1%
82.	https://www.cybercompex.org/member-cp/private-messages	10	0.1%	7	0.7%	70	0.0%
83.	https://www.cybercompex.org/category/default-category	10	0.1%	6	0.6%	163	0.1%
84.	https://www.cybercompex.org/member-cp/update-profile/redirect/https%3A%2F%2Fwww.cybercompex.org%2Fmember-cp%2Fprivate-messages	10	0.1%	4	0.4%	528	0.3%
85.	desktop|ccx|jpw|/jpw/jobs/jobpostingdetailsoptions.aspx	10	0.1%	2	0.2%	2,094	1.0%
86.	https://cybercompex.org/topic/cybrary-report-data-security-still-hampered-by-lack-of-talent	9	0.1%	8	0.8%	660	0.3%
87.	https://www.cybercompex.org/event/executive-women-s-forum-cyber-security-schoolchallenge	9	0.1%	8	0.8%	562	0.3%
88.	https://www.cybercompex.org/g/sans/join	9	0.1%	8	0.8%	40	0.0%
89.	desktop|ccx|hiring|/modules/account/createaccount.aspx	9	0.1%	7	0.7%	2,839	1.3%
90.	https://www.cybercompex.org/topic/this-is-terrifying	9	0.1%	7	0.7%	163	0.1%
91.	https://www.cybercompex.org/forum/cyber-9-12-project	9	0.1%	7	0.7%	47	0.0%
92.	https://www.cybercompex.org/topic/honeynet-project-challenges	9	0.1%	6	0.6%	279	0.1%
93.	desktop|ccx|mgs|/channels/mgs1000/dashboard.aspx	9	0.1%	6	0.6%	66	0.0%
94.	https://www.cybercompex.org/topic/waspnet-ctf	9	0.1%	5	0.5%	1,100	0.5%
95.	desktop|ccx|hiring|/account/createaccountthankyou.aspx	9	0.1%	4	0.4%	1,448	0.7%
96.	https://www.cybercompex.org/topic/cyber-9-12-project	8	0.1%	8	0.8%	536	0.3%
97.	https://www.cybercompex.org/event/2016-cyber-security-brainstorm	8	0.1%	8	0.8%	133	0.1%
98.	https://www.cybercompex.org/forum/competition-metric-guidelines	8	0.1%	7	0.7%	55	0.0%
99.	https://www.cybercompex.org/login/context/GENERAL/redirect/https%3A%2F%2Fwww.cybercompex.org%2Fmember-cp%2Fupdate-profile	8	0.1%	5	0.5%	292	0.1%
100.	https://www.cybercompex.org/forum/ewf-cyber-security-school-challenge	8	0.1%	5	0.5%	39	0.0%
	Total	7,345		1,001		210,870	

US Cyber Challenge (USCC)

2016 Camp Analysis

www.uscyberchallenge.org

25 October 2016

Table of Contents

Introduction

In 2016 the USCC hosted cyber security camps in multiple locations across the United States. These camps provided high school, college, and young professionals with one week of specialized cyber security training presented by college faculty and cyber security experts, and include a job fair and/ or capture-the-flag competition at the various camps.

2016 Camp Schedule

- *Delaware State University (DE), July 11th through July 15th*
  - Day 1 General Penetration Testing
  - Day 2 Introduction to Network Penetration Testing
  - Day 3 Web App Ethical Hacking
  - Day 4 Metasploit Kung Fu for Penetration Testers
  - Day 5 Capture the Flag
- *Moraine Valley Community College (MV), July 20th through July 24th*
  - Day 1 Introduction to Network Penetration Testing
  - Day 2 Metasploit Kung Fu for Penetration Testers
  - Day 3 Web App Penetration Testing
  - Day 4 Packet Crafting with Scapy
  - Day 5 Capture the Flag
- *Southern Utah University (SUU), July 27th through July 31st*
  - Day 1 Introduction to Network Penetration Testing
  - Day 2 Web App Ethical Hacking
  - Day 3 Metasploit Kung Fu for Penetration Testers
  - Day 4 Packet Crafting with Scapy
  - Day 5 Capture the Flag

The Cyber Camps provide crucial skills development and enable USCC to tap into the tremendous talent across our nation to identify those with a passion for security and a desire to put their skills to good use in addressing our Nation's cyber security workforce challenges. In addition to providing expert training for participants to improve their skills and marketability, the Cyber Camps provided attendees the opportunity to engage with major technology companies

and government agencies at onsite job fairs for scholarship, internship and employment opportunities as well as engage industry professionals in an ethics panel.

This report provides an overview of the feedback collected from camp surveys, a summary of findings from interviews with camp administrators, TAs and instructors, a summary of overarching observations derived from those interviews, as well as general recommendations for future camps.

Survey Structures

2016 Survey Structures

In 2016, feedback on presenters and instructors was collected from participants using the CyberCompEx collaboration platform. The *2016 USCC Evaluation Survey* (or simply *Evaluation Survey*), was given to participants to evaluate the setup, execution, and expectations for the event.

2016 USCC Evaluation Survey Structure

1. Course Evaluation

1.1. On a scale of 1-10, what is your overall evaluation of this course?

1.1.1. 1, Bad
1.1.2. 2,
1.1.3. 3, Poor
1.1.4. 4,
1.1.5. 5, Marginal
1.1.6. 6,
1.1.7. 7, Good
1.1.8. 8,
1.1.9. 9, Great
1.1.10. 10, Excellent

1.2. On a scale of 1-10, what is your overall evaluation of the instructor's teaching skill?

1.2.1. 1, Bad
1.2.2. 2,
1.2.3. 3, Poor
1.2.4. 4,
1.2.5. 5, Marginal
1.2.6. 6,
1.2.7. 7, Good
1.2.8. 8,
1.2.9. 9, Great

1.2.10. 10, Excellent

1.3. On a scale of 1-10, what is your overall evaluation of the value of the course?

1.3.1. 1, Bad

1.3.2. 2,

1.3.3. 3, Poor

1.3.4. 4,

1.3.5. 5, Marginal

1.3.6. 6,

1.3.7. 7, Good

1.3.8. 8,

1.3.9. 9, Great

1.3.10. 10, Excellent

1.4. If you have any additional comments or feedback, please provide it here.

1.4.1. Free form data entry.

2. Capture the Flag Evaluation

2.1. Were the TAs helpful in explaining the set up for this event?

2.1.1. Yes

2.1.2. No

2.2. On a scale to 1-5, how would you rate the quality of the technical documentation, if any provided by the TAs?

2.2.1. 1, Inadequate

2.2.2. 2, Poor

2.2.3. 3, Acceptable

2.2.4. 4, Good

2.2.5. 5, Excellent

2.3. Did the competition appear to provide the technical challenge for the class?

2.3.1. Yes

2.3.2. No

2.4. Do you fell the technical set up was easy to achieve?

2.4.1. Yes

2.4.2. No

2.5. Did the technical performance meet your expectations?

2.5.1. Yes

2.5.2. No

2.6. On a scale of 1-10, what is overall evaluation of this event?

2.6.1. 1, Bad

2.6.2. 2

2.6.3. 3, Poor

2.6.4. 4

2.6.5. 5, Marginal

2.6.6. 6

2.6.7. 7, Good

2.6.8. 8

2.6.9. 9, Great

2.6.10. 10, Excellent

2.7. What are the strengths of this competition?

2.7.1. Free form data entry.

2.8. What are the areas for improvements for this competition?

2.8.1. Free form data entry.

2.9. Would you recommend this competition to your peers?

2.9.1. Yes

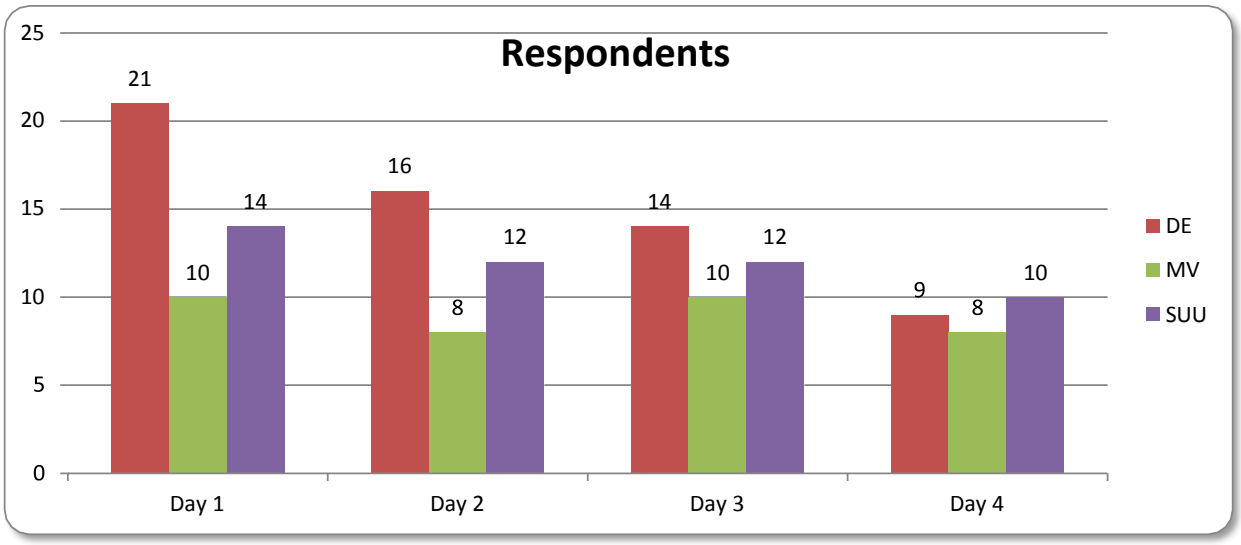
2.9.2. No

2.10. If you have any additional comments or feedback, please provide it here

2.10.1. Free form data entry.

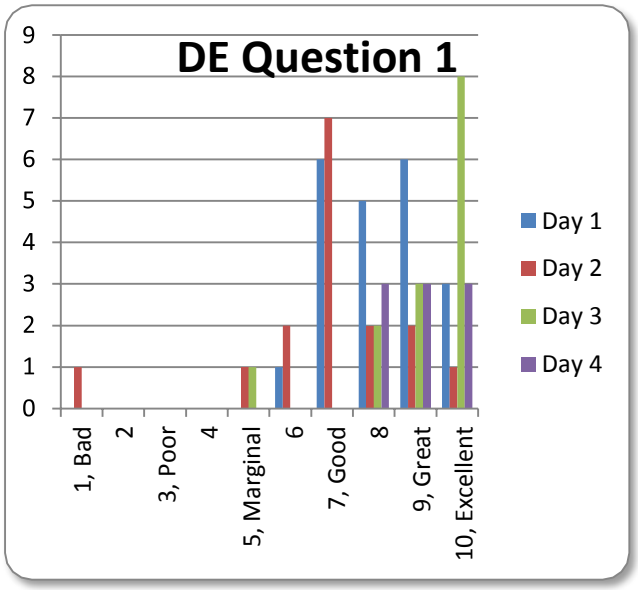
Comprehensive Course Analysis Results

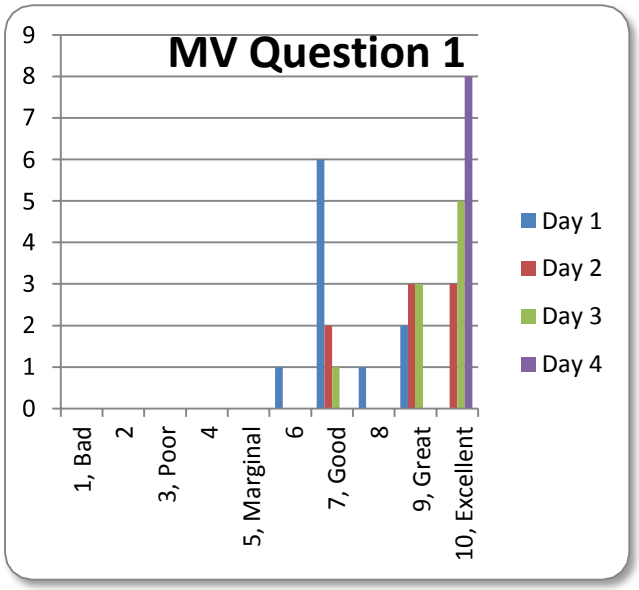
Number of Respondents

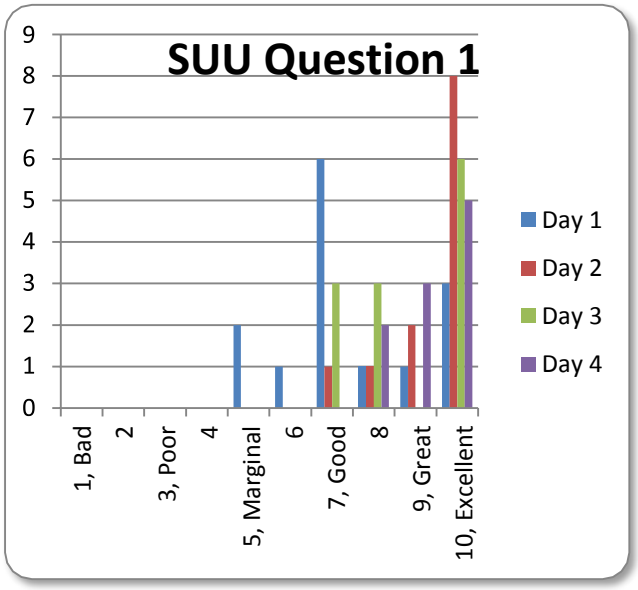


Respondent Summary			
	DE	**MV**	**SUU**
Day 1	21	10	14
Day 2	16	8	12
Day 3	14	10	12
Day 4	9	8	10

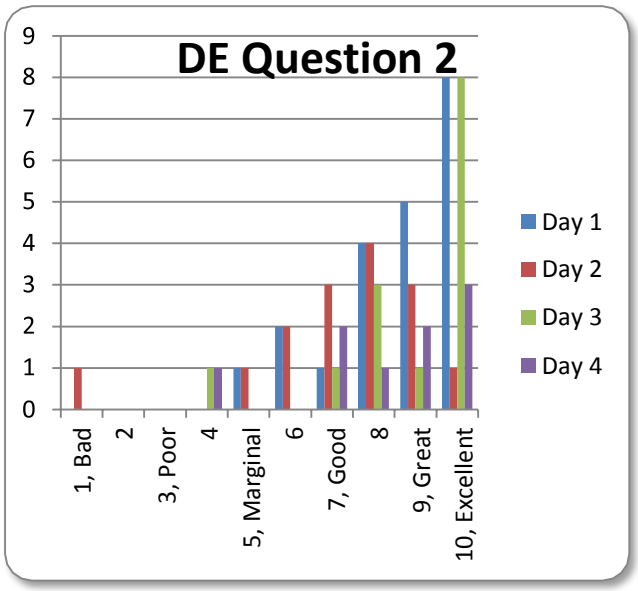
On a scale of 1-10, what is your overall evaluation of this course?

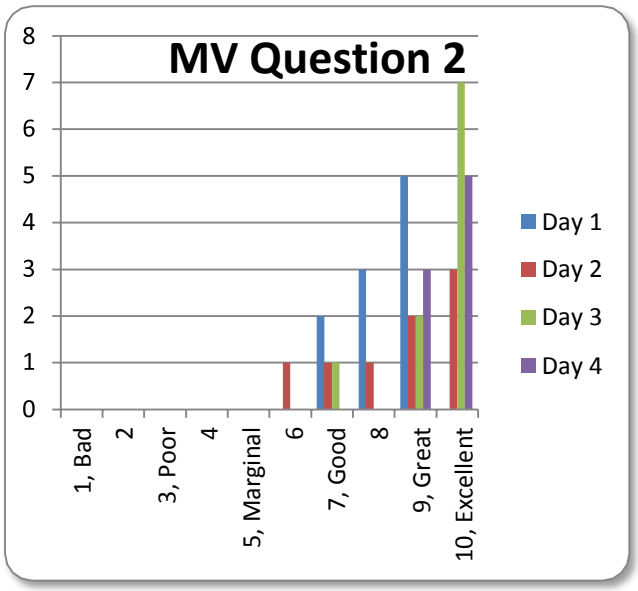


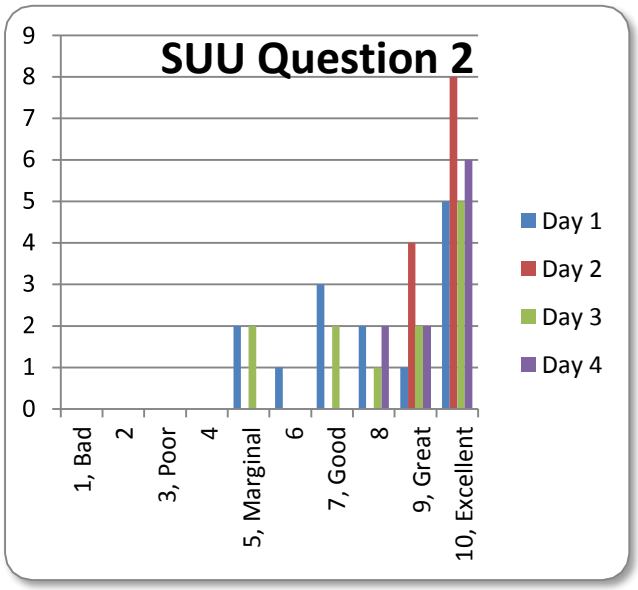




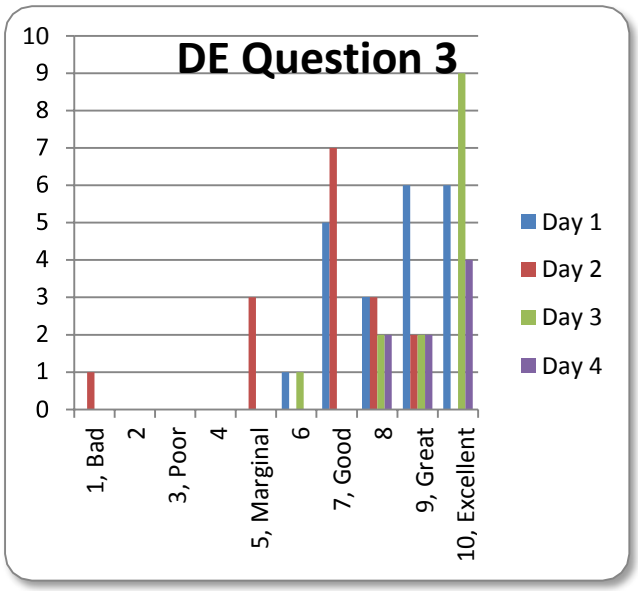
On a scale of 1-10, what is your overall evaluation of the instructor's teaching skill?

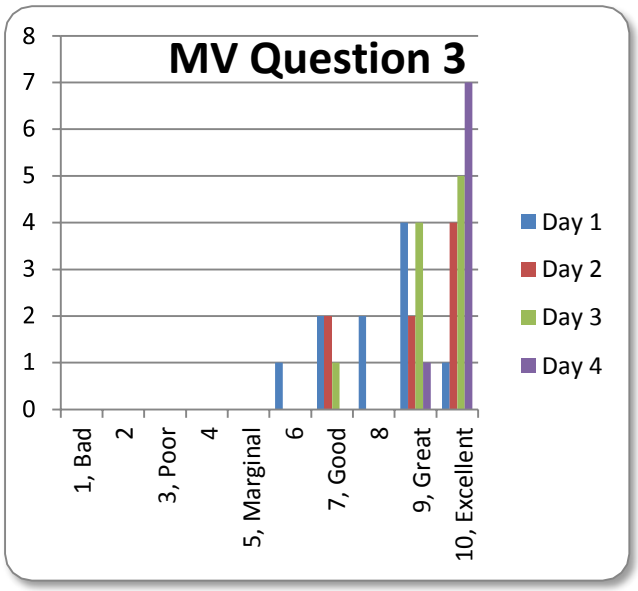


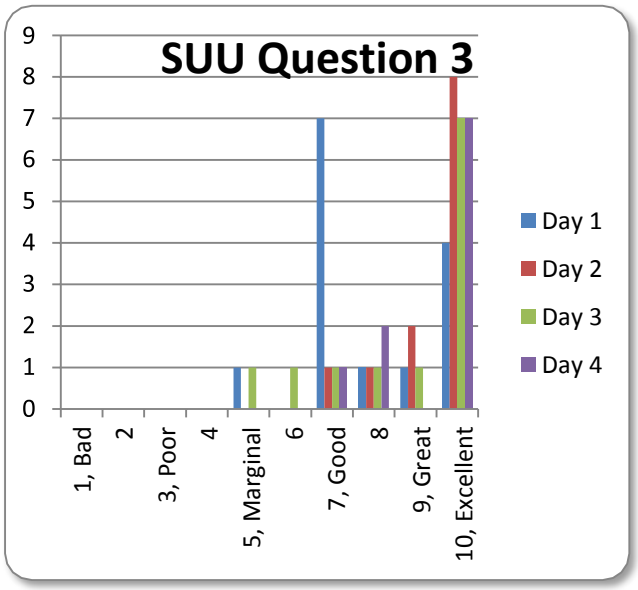




On a scale of 1-10, what is your overall evaluation of the value of the course content?

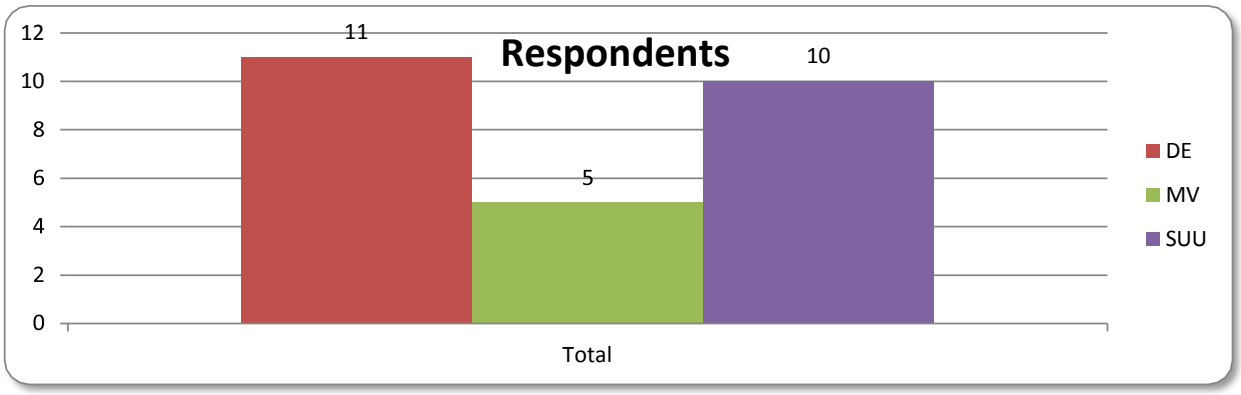






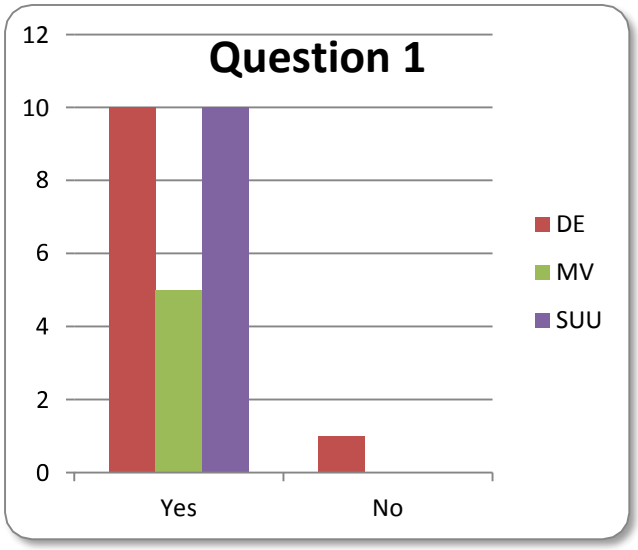
Comprehensive CTF Analysis Results

Number of Respondents

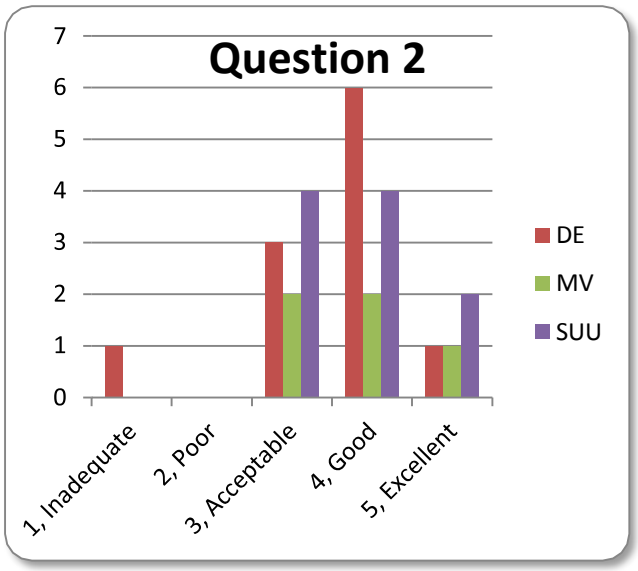


Respondent Summary			
	DE	**MV**	**SUU**
Total	11	5	10

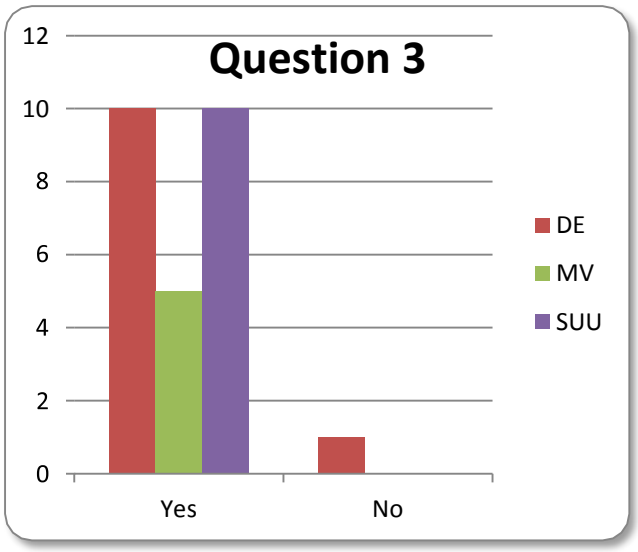
Were the TAs helpful in explaining the set up for this event?



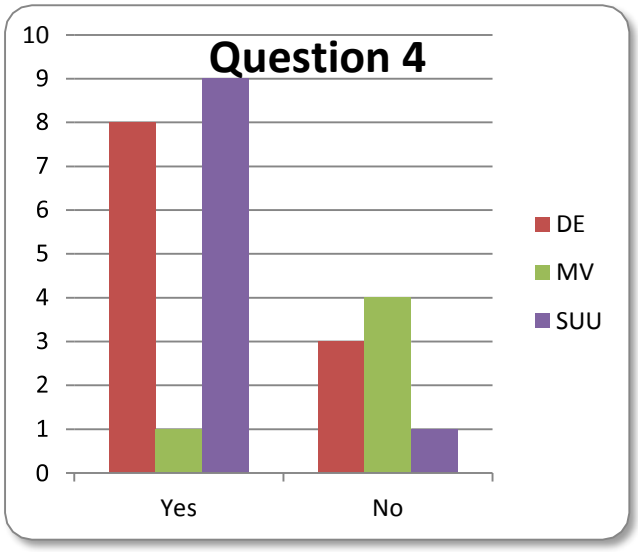
On a scale to 1-5, how would you rate the quality of the technical documentation, if any provided by the TAs?



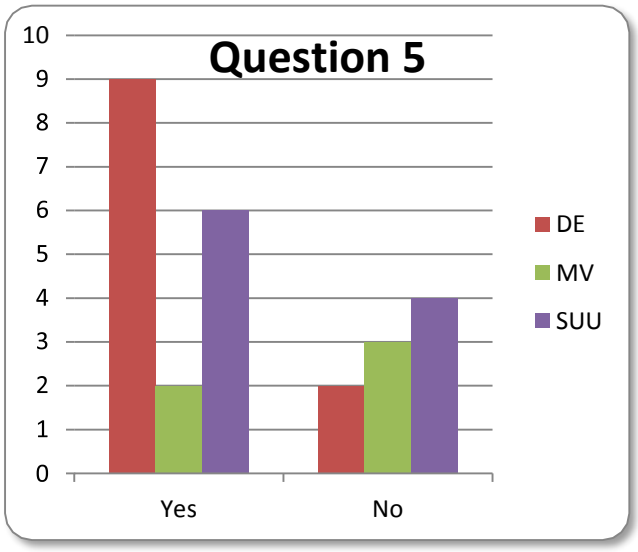
Did the competition appear to provide the technical challenge for the class?



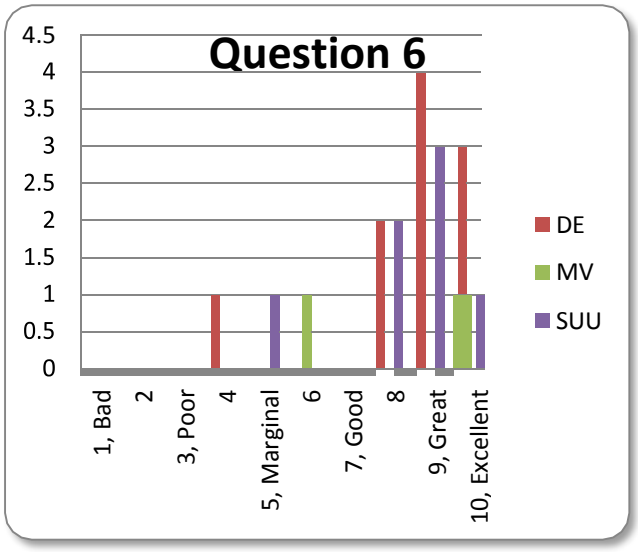
Do you fell the technical set up was easy to achieve?



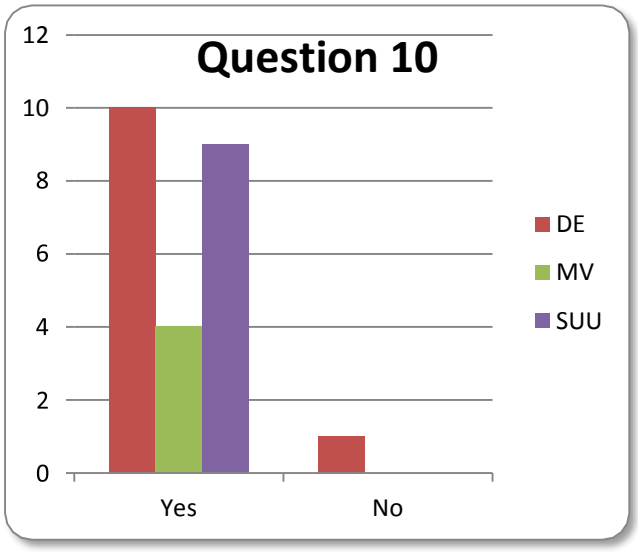
Did the technical performance meet your expectations?



On a scale of 1-10, what is overall evaluation of this event?



Would you recommend this competition to your peers?



List of Acronyms

AFFIRM	The Association for Federal Information Resources Management
CCX	CyberCompEx.org
Multi-State ISAC	Multi-State Information Sharing and Analysis Center
CSIS	Center for Strategic and International Studies
CTF	Capture the Flag
Multi-State ISAC	Multi-State Information Sharing and Analysis Center
TAs	Teaching Assistants
USCC	United States Cyber Challenge